JC10 Rec'd PCT/PTO 12 MAR 2002

FORM PTO-1390 (REV. 10-96)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY DOCKET NUMBER
	TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371	A-71400/DJB/MAK
		U.S. APPLICATION NO. (If known, sect 37 C.F.R. 1.5) Not Yet Known 10/088034

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/AU00/01095	13 September 2000	13 September 1999

TITLE OF INVENTION

AN ACCESS CONTROL METHOD

APPLICANT(S) FOR DO/EO/US

Timothy Winston HIBBERD

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau. **(see enclosed Form PCT/IB/308)**
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information.

JC13 Rec'd PCT/PTO 12 MAR 2002

APPLICATION NO. (If known, see 37 C.F.R. 1.53)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
Not Yet Known 10/088034	PCT/AU00/01095	A-71400/DJB/MAK

17. ☒ The following fees are submitted:	CALCULATIONS (PTO USE ONLY)
Basic National Fee (37 CFR 1.492(a)(1)-(5)):	
Search Report has been prepared by the EPO or JPO $890.00	
International preliminary examination fee paid to USPTO (37 CFR 1.482) $710.00	
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $740.00	
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1,040.00	
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 1,040.00
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☒ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ 130.00

CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE	
Total Claims	18	-20 =	0	$ 18.00	$ 0.00
Independent Claims	3	-3 =	0	$ 84.00	$ 0.00
Multiple dependent claims (if applicable)				$280.00	$ 0.00

TOTAL OF ABOVE CALCULATIONS =		$ 1,170.00
Reduction by 1/2 for filing by small entity, if applicable. Applicant claims small entity status. (See 37 CFR 1.27.)	Yes / No	$ 0.00
SUBTOTAL =		$ 1,170.00
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +		$
TOTAL NATIONAL FEE =		$ 1,170.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +		$
TOTAL FEES ENCLOSED =		1,170.00
	Amount to be: refunded	$
	charged	$

a. ☒ A check in the amount of $ 1,170.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. 06-1300 (Order No. _____) in the amount of $ _____ to cover the above fees.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-1300 (Order No. A-71400/DJB/MAK).

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Michael A. KAUFMAN
FLEHR HOHBACH TEST
ALBRITTON & HERBERT LLP
Four Embarcadero Center - Suite 3400
San Francisco, California 94111-4187
Tel.: (415) 781-1989
Fax: (415) 398-3249

Michael A. Kaufman
SIGNATURE

Michael A. KAUFMAN
NAME

32,998
REGISTRATION NUMBER

10/088034
JC13 Rec'd PCT/PTO 12 MAR 2002

PATENT

Attorney Docket No.: A-71400/DJB/MAK

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Timothy Winston HIBBERD

NATIONAL PHASE ENTRY OF:
PCT/AU00/01095

Serial No.: Not Yet Assigned

Filing Date: Herewith

For: ***An Access Control Method***

Box PCT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

FIRST PRELIMINARY AMENDMENT

Sir:

This Preliminary Amendment accompanies the filing of an application under 35 U.S.C. § 371.

Prior to examination, please amend the above-identified application as follows:

IN THE CLAIMS:

Claims 1-6, 8, 9, 11-15 and 18 are to remain unchanged. Please replace claims 7, 10, 16 and 17 with the following rewritten claims. Replacement claims pages 10-13 are appended hereto and incorporate the following rewritten claims.

7. An access control method as claimed in claim 2, wherein said at least one additional level of access control includes sending communication

software to said apparatus to receive access requests for said service under an additional communication protocol.

10. An access control method as claimed in claim 6, wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol and wherein said verifying of said identification data is a first level of access control, said detecting is a second level of access control, and said sending of said communication software and execution of said additional communication protocol is a third level of access control.

16. An access control system having components for executing the steps of the access control method as claimed in claim 1.

17. Access control software stored on a computer system, having code for executing the steps of the access control method as claimed in claim 1.

IN THE ABSTRACT OF THE DISCLOSURE:

Please add the following new paragraph and heading at the top of new page 14. New page 14 is appended hereto and incorporates the following new text.

ABSTRACT

An access control method executed by a computer system, including applying an access rate limit until a user issuing access requests is verified, a first control level involving verifying the user, a second control level applying hack program detection tests to the access requests and verifying the user, a third control level requiring use of predetermined download software for transmitting

PCT Appl. No.: PCT/AU00/01095
U.S. Serial No.:: Not Yet Known
U.S. Filing Date: Herewith

the access requests and verifying the user, a fourth control level blocking access to the service on the basis of at least one communications address corresponding to the access requests, and invoking the control levels sequentially depending on a number of failed attempts to verify the user.

REMARKS

The foregoing claim amendments are made to obviate the problem of improper dependency in the multiple dependent claims which existed in the PCT priority document. The foregoing abstract of the disclosure was added because no abstract appeared in the PCT priority document. Appended hereto at page 4 is a marked-up version of the foregoing amendments in which additions to the text are shown with a gray background and deletions with .

The Commissioner is authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-1300 (Our Order No. A-71400/DJB/MAK).

Respectfully submitted,

FLEHR, HOHBACH, TEST,
ALBRITTON & HERBERT LLP

Dated: 12 March 2002

By: Michael A. Kaufman
Michael A. KAUFMAN
Reg. No. 32,998
Attorneys for Applicants

Embarcadero Center - Suite 3400
San Francisco, California 94111-4187
Tel.: (415) 781-1989
Fax: (415) 398-3249

SF-1077326v1

PCT Appl. No.: PCT/AU00/01095
U.S. Serial No.:: Not Yet Known
U.S. Filing Date: Herewith

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

Claims 7, 10, 16 and 17 have been amended as follows:

7. An access control method as claimed in claim 2 ~~or 6~~, wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol.

10. An access control method as claimed in claim ~~7 6, when dependent on claim 6,~~ wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol and wherein said verifying of said identification data is a first level of access control, said detecting is a second level of access control, and said sending of said communication software and execution of said additional communication protocol is a third level of access control.

16. An access control system having components for executing the steps of the access control method as claimed in claim 1 ~~any one of the preceding claims~~.

17. Access control software stored on a computer system, having code for executing the steps of the access control method as claimed in ~~any one of~~ claims 1 ~~to 15~~.

IN THE ABSTRACT OF THE DISCLOSURE:

The following text has been added as an abstract of the disclosure:

ABSTRACT

An access control method executed by a computer system, including applying an access rate limit until a user issuing access requests is verified, a first control level involving verifying the user, a second control level applying hack program detection tests to the access requests and

PCT Appl. No.: PCT/AU00/01095
U.S. Serial No.: Not Yet Known
U.S. Filing Date: Herewith

verifying the user, a third control level requiring use of predetermined download software for transmitting the access requests and verifying the user, a fourth control level blocking access to the service on the basis of at least one communications address corresponding to the access requests, and invoking the control levels sequentially depending on a number of failed attempts to verify the user.

CLAIMS:

1. An access control method, including:

receiving an initial access request for a service from a data processing apparatus;

sending unique identification data to said apparatus in response to said initial access request; and

applying a rate limit for verifying access to said service until said identification data is verified by a user of said apparatus.

2. An access control method as claimed in claim 1, wherein verifying said identification data corresponds to a first level of access control, and said method includes applying at least one additional level of access control following a predetermined number of failed attempts to verify said identification data by said user of said apparatus.

3. An access control method as claimed in claim 2, wherein said identification data is a random unique security code and said apparatus is sent an unique identification number which expires if the security code is not verified within a predetermined period of time.

4. An access control method as claimed in claim 1, wherein said identification data is verified by contacting a device with a known association to said user and said data processing apparatus, and having said user provide said identification data using said device.

5. An access control method as claimed in claim 1, wherein said identification data is verified by said user returning said identification data using communication means having a known association to said user and said data processing apparatus.

6. An access control method as claimed in claim 2, wherein said at least one additional level includes detecting generation of access requests for said service under control of a program instead of under control of said user.

7. An access control method as claimed in claim 2, wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol.

8. An access control method as claimed in claim 7, wherein said communication software encrypts said access requests.

9. An access control method as claimed in claim 2, including invoking sequentially the levels of access control depending on the number of failed attempts to verify said identification data by said user for access requests over predetermined periods of time.

10. An access control method as claimed in claim 6, wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol and wherein said verifying of said identification data is a first level of access control, said detecting is a second level of access control, and said sending of said communication software and execution of said additional communication protocol is a third level of access control.

11. An access control method as claimed in claim 10, wherein said at least on additional level of access control includes a fourth level of access control involving blocking all access requests by said data processing apparatus.

12. An access control method as claimed in claim 11, wherein said blocking involves denying all access requests that include address data that corresponds to said data processing apparatus.

13. An access control method as claimed in claim 12, wherein the address data is an IP address or segment.

14. An access control method executed by a computer system, including:

applying an access rate limit until a user issuing access requests is verified;

a first control level involving verifying said user;

a second control level applying hack program detection tests to said access requests and verifying said user;

a third control level requiring use of predetermined download software for transmitting said access requests and verifying said user;

a fourth control level blocking access to said service on the basis of at least one communications address corresponding to said access requests; and

invoking said control levels sequentially depending on a number of failed attempts to verify said user.

15. An access control method as claimed in claim 14, wherein said user is verified by contacting a device with a known association to said user and said data processing apparatus, and having said user provide identification data using said device.

16. An access control system having components for executing the steps of the access control method as claimed in claim 1.

17. Access control software stored on a computer system, having code for executing the steps of the access control method as claimed in claim 1.

18. An access control system, including:

an access control server for receiving access requests for a service from a data processing apparatus, rate limiting access to the server until a user of said apparatus is verified, and sending to said data processing apparatus unique identification data; and

an IVR for contacting a device having an association with said data processing apparatus, issuing a request for said identification data, and providing the data received in response to said request to said access server in order to verify said user.

ABSTRACT

An access control method executed by a computer system, including applying an access rate limit until a user issuing access requests is verified, a first control level involving verifying the user, a second control level applying hack program detection tests to the access requests and verifying the user, a third control level requiring use of predetermined download software for transmitting the access requests and verifying the user, a fourth control level blocking access to the service on the basis of at least one communications address corresponding to the access requests, and invoking the control levels sequentially depending on a number of failed attempts to verify the user.

AN ACCESS CONTROL METHOD

The present invention relates to an access control method and to a system and a computer program for executing the method.

One of the perennial problems with providing services over a communications network, such as the Internet, is the vulnerability of the system providing the service to damage or attack by malicious parties, such as computer hackers. Particularly for service provision over the Internet, services, such as information provision and communication services, may be accessed using scripts or applets which the hackers can attempt to replicate in programs to execute excessive access requests for the service. The excessive access requests, depending on their nature, can have a variety of effects on the service and in some circumstances may cause the service system to collapse.

Detecting a spurious access request or "hack" by a hacker is problematic for any service provider and a considerable number of security procedures have been developed to try and protect systems from a hack. Hackers however have proven particularly adept at being able to circumvent all forms of security procedures and systems which seek to deny them access. Given the computing resources and skills which the hacking community possess, an alternative approach to protecting service provision systems is needed.

In accordance with the present invention there is provided an access control method, including:

receiving an initial access request for a service from a data processing apparatus;

sending unique identification data to said apparatus in response to said initial access request; and

applying a rate limit for verifying access to said service until said identification data is verified by a user of said apparatus.

The present invention also provides an access control method executed by a computer system, including:

applying an access rate limit until a user issuing access requests is verified;

a first control level involving verifying said user;

a second control level applying hack program detection tests to said access requests and verifying said user;

a third control level requiring use of predetermined download software for transmitting said access requests and verifying said user;

a fourth control level blocking access to said service on the basis of at least one communications address corresponding to said access requests; and

invoking said control levels sequentially depending on a number of failed attempts to verify said user.

The present invention also provides an access control system having components for executing the steps of the method.

The present invention also provides an access control software stored on a computer system, having code for executing the steps of the access control method

The present invention also provides an access control system, including:

an access control server for receiving access requests for a service from a data processing apparatus, rate limiting access to the server until a user of said apparatus is verified, and sending to said data processing apparatus unique identification data; and

an IVR for contacting a device having an association with said data processing apparatus, issuing a request for said identification data, and providing the data received in response to said request to said access server in order to verify said user.

A preferred embodiment of the present invention is hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram of a preferred embodiment of an access control system connected to a communications network.

An access control system 2, as shown in Figure 1, is used to limit access to and protect a service provision system 4. The access control system 2 includes an access control server 6 and an interactive voice response system (IVR) 8 which are both connected to a communications network 30 and to each other. The service system 4 includes a network server 10 connected to the access server 6, and an application server 12 connected to the network server 10 and having access to a database 14. The application server 12 executes the application to provide a service over the network 30 using the data contained in the database 14. The application server 12 gains access to the network 30 via the network server 10, which may be a web server to handle communications with the network using HTTP. The access server 6 is also able to communicate with the network 30 using HTTP and other protocols as necessary. The network 30 includes the Internet and other data and voice delivery networks, such as a public switched telephone network (PSTN). Although the servers 6, 10 and 12 and the IVR 8 are shown as separate machines, the machines can be integrated into one machine or divided into different machines which may be distributed and communicate remotely, as will be understood by those skilled in the art. The latter involves distributing the software components of the servers 6, 10 and 12 and the IVR 8 amongst the different machines.

The preferred embodiment is described below with reference to the provision of a service for executing icon calling, where the application server 12 allows parties (an A party) using a data processing apparatus 22 (i.e. a computer) to access directory or telephone information concerning another party (the B party) via a web site, and then select a call icon on a page of the site to establish a call between the A and B parties. This involves the application server 12 instructing the network 30 to place a call to a telephone 16 of the A party and a telephone 18 or 20 of the B party. Further details concerning the system required to support the service is provided in the applicant's Australian Patent Application No. 19173/97. It will of course be apparent to a skilled addressee that the access control method executed by the system 2 described below can be applied to any service delivered over the communications network 30.

The access control method is executed by a computer program stored on the access control server 6 which communicates with and uses the standard features of the IVR 8, such as those provided with the IVRs produced by Periphonics Corporation or Dialogic Corporation. Again, the program could be distributed or its processes executed by dedicated hardware, such as application specific integrated circuits (ASICs), as will be understood by those skilled in the art.

The access control method adopts a different approach to standard security methods, in that it is assumed that a hacker using the apparatus 22 will eventually be able to penetrate any defences, and therefore allows legitimate users to use the system 4 whilst it is under attack. The method seeks to limit the number of access requests for the service that a hacker can make whilst moving through different control levels as the number of access attempts increase over monitored periods of time. For the icon calling service this means limiting the number of prank calls to the same as that which could be made from a telephone. In other words, this involves rate limiting the number of requests to the same level at which call requests could be made from a telephone. Whilst the access limit is in place, if a user is not verified, the control levels will move through a second hack detection level, a third software download level and a fourth level where access is completely blocked for the apparatus 22.

The data processing apparatus 22 does not provide any unique identification (ID) when making an access request to the system 4 which can be used by the access control system 2, because an IP address is not unique for a machine 22 which is sharing a proxy server with other machines. The method therefore involves creating an ID which is stamped on the requesting machine 22. Supplementary information delivery strategies currently supported by web browsers are cookie files and Secured Sockets Layer (SSL) client certificates, but as the availability of client certificates cannot be relied upon, the method uses encrypted cookie files, as described below. The A party user or the telephone 16 of the requesting A party is verified by executing an IVR based security check. The access control server 6 instructs the IVR 8 to place a call to the telephone 16 designated in the call request, and the answering party is asked to enter or divulge a unique code which is sent to the machine 22 for display by the access control server 6. The IVR 8 then reports

back to the server 6 the code provided using the telephone 16. If the sent and received security codes correspond the A party is verified. A rate limit is therefore applied to a request having an IP address identifying the machine 22 until this IVR verification has been successfully completed.

The control levels of the access control method described below apply to unverified A party numbers from a given IP address. If *m* or more IP addresses in a segment are operating under a control level (m being an integer greater than or equal to 2), an entire IP segment, i.e. 256 addresses, is tagged as being in a control level. This provides protection from a hacker who is cycling through IP addresses in a segment. However, it is not until the fourth control level is reached that any IP address or segment blocking occurs, as this is potentially serious given that an entire proxy server can be blocked.

The first control level rate limits access requests so that the service is not denied to legitimate users and the telephone network is not adversely affected. At this level, the access method executes the IVR based verification or validation check, which additionally ensures that a computer 22 has been configured correctly.

When an initial access request is made by the data processing apparatus 22, the access control system 6 treats this initial access request as a request to register with the system 4 and enters a registration validation procedure where a time-limited encrypted cookie file encoded with a unique identification number is sent for storage at the machine 22 and can be used to make one call. When the A party is called for the first time, a random unique security code, which in this instance can be text based, is sent for display on the computer 22 and the IVR 8 is instructed by the access control system 6 to provide a prompt for the answering party at the telephone 16 to provide the displayed security code. If the security code is entered correctly by the answering party, using DTMF signals generated by pressing the buttons on the telephone 16, the time limit in the encrypted cookie is cancelled and the number of calls that can be made is changed to unlimited. The B party is then called on the telephone 18 or 20. Once the security code is verified the identification number in the cookie is sent with access requests to the application system 4.

The following rate limits are continuously imposed by the access control server 6 for unverified access requests:

1. One concurrent call per machine identification (ID), which is the preferred cookie ID rather than a SSL certificate ID.
2. One concurrent call per A party 16, identified by the A party number.
3. X concurrent calls per access system 2, which is the number of concurrent calls the system 2 is able to support.
4. One concurrent A party IVR validation procedure for a given IP address or segment.

Access requests or call requests that are received that exceed the above rate limits are queued by the access system 2 and a user is presented with their position in the queue on a page sent to the web browser of the user's machine 22. The queue position display also includes expected time in the queue. A configurable queue size limit applies to each requesting IP address to prevent overuse of system resources.

The IVR validation check procedure is considered to have failed if an A party call is invalidated in that the call enters a ringing state and is abandoned or is connected and disconnected without the correct security code being entered into the telephone. This may occur if a requesting party at the machine 22 enters an A party number which is not theirs and a telephone 18 or 20 is rung which is not associated with the machine 22. The person who receives this call of course cannot see the displayed security code on the screen of the machine 22. Essentially this will be a prank A party call.

The above procedures of the first security level, in particular the rate limit (no. 5) regarding concurrent registration and the time limit in the cookie, essentially eliminate any prank B party calls and limit the number of prank A party calls to about 2 to 6 per minute. The additional protection procedures in the additional control levels below limit the number of prank A party calls further so that only a few calls can be made.

The second access control level is entered if an IP address or segment fails a predetermined number, say *n*, IVR verifications or checks within the last 24 hours. The default for *n* would be 2. The purpose of this level is to execute additional tests on the user to ensure that a person is controlling the machine 22 and generating the access requests, as opposed to an automated program or hack. The tests in this level do not require the user to download any software to their computer 22.

The tests which are executed include the following:

1. A security code is again sent by the access control server 6 to the machine 22 for display and the IVR 8 instructed to call the A party telephone 16 and prompt for the security code to be entered. In this instance, however, the security code is presented in a graphic format, i.e. as a bitmap image. This will defeat any automated program which is simply looking for the code in a text based format, and will require any hacker to adjust the hacking program to incorporate optical character recognition which is sufficiently accurate to extract the security code.
2. Script or an applet is sent from the access control system to the machine 22 which is configured to scan the machine to detect an automatic continually iterative hacking program which may be making the access requests. This could be detected by a hacker.
3. The access control system 6 runs a check procedure to determine whether the HTTP requests from the machine 22 include data associated with normal use of most browsers, such as Netscape Navigator™ and Microsoft Internet Explorer™, and which would not normally be returned by a hacking program.
4. A time based test is executed also by the access control server 6 to detect whether the access requests are made faster than would be possible if the machine 22 was under human control.

Other remote checks for program control can also be executed.

This control level reduces the attack rate further by forcing a hacker to consider how to meet the above tests. This will take some time, believed to be at least 24 hours.

An IP address or segment at this control level will return to the first control level within 24 hours if no additional IVR verification failures occur. This will ensure that IP addresses randomly assigned by an Internet service provider (ISP) are not blocked simply because a hacker has generated a few prank calls.

The third access control level is entered if an IP address or segment fails *o* IVR tests, within 24 hours from the first access request, where *o* is greater than *n*.

In this control level, the access control server 6 sends a prompt to the user's machine 22 to download software to the machine 22. When a request for the software is received, the access control server 6 sends the software which, when stored on the machine 22, ensures all future communications between the machine 22 and the systems 2 and 4 is executed using a secure encrypted communications protocol. This prevents a hacker from determining the data passed between the machine 6 and the access control server 6 in all future communications. It also allows the downloaded software to examine the user's machine 22 and send investigative data securely back to the access control system 6 to detect if a person or program is controlling the machine 22. Again, a hacker, after some time, may be able to break the encrypted communication protocol and create a wrapper program which mimics the downloaded software so that the hack can continue using the protocol to access the system 4. Again the time needed to break this control level is assumed to be at least 24 hours.

A machine 22 at the third control level returns to the first control level status within 48 hours from the initial access request if no additional IVR check failures occur. This is done, as mentioned previously, to allow release of IP addresses randomly assigned by ISPs.

An IP address or segment will reach the fourth control level and remain in this state until manually cleared by an operator of the system 2 if the IP address or segment has

failed o+1 IVR checks. This level is used to block the IP address or segment which is considered to be unverified. All access requests from the IP address or segment is refused. The block is made as close as possible to the machine 22, preferably at a router level, in the network 30 to reduce the performance impact of a continuous attack. Accordingly the attack is reduced further by blocking the IP address or segment as close as possible to where the attack originates, which can block an entire proxy server.

The access control server 6 executes a reverse Domain Name Server (DNS) lookup procedure to determine the manager of the domain associated with the IP address or segment and then sends an e-mail message to the manager advising the block has occurred. A copy of the e-mail is also sent to inform the operator of the systems 2 and 4.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described with reference to the accompanying drawing.

CLAIMS:

1. An access control method, including:

receiving an initial access request for a service from a data processing apparatus;

sending unique identification data to said apparatus in response to said initial access request; and

applying a rate limit for verifying access to said service until said identification data is verified by a user of said apparatus.

2. An access control method as claimed in claim 1, wherein verifying said identification data corresponds to a first level of access control, and said method includes applying at least one additional level of access control following a predetermined number of failed attempts to verify said identification data by said user of said apparatus.

3. An access control method as claimed in claim 2, wherein said identification data is a random unique security code and said apparatus is sent an unique identification number which expires if the security code is not verified within a predetermined period of time.

4. An access control method as claimed in claim 1, wherein said identification data is verified by contacting a device with a known association to said user and said data processing apparatus, and having said user provide said identification data using said device.

5. An access control method as claimed in claim 1, wherein said identification data is verified by said user returning said identification data using communication means having a known association to said user and said data processing apparatus.

6. An access control method as claimed in claim 2, wherein said at least one additional level includes detecting generation of access requests for said service under control of a program instead of under control of said user.

7. An access control method as claimed in claim 2 or 6, wherein said at least one additional level of access control includes sending communication software to said apparatus to receive access requests for said service under an additional communication protocol.

8. An access control method as claimed in claim 7, wherein said communication software encrypts said access requests.

9. An access control method as claimed in claim 2, including invoking sequentially the levels of access control depending on the number of failed attempts to verify said identification data by said user for access requests over predetermined periods of time.

10. An access control method as claimed in claim 7 when dependent on claim 6, wherein said verifying of said identification data is a first level of access control, said detecting is a second level of access control, and said sending of said communication software and execution of said additional communication protocol is a third level of access control.

11. An access control method as claimed in claim 10, wherein said at least on additional level of access control includes a fourth level of access control involving blocking all access requests by said data processing apparatus.

12. An access control method as claimed in claim 11, wherein said blocking involves denying all access requests that include address data that corresponds to said data processing apparatus.

13. An access control method as claimed in claim 12, wherein the address data is an IP address or segment.

14. An access control method executed by a computer system, including:

applying an access rate limit until a user issuing access requests is verified;

a first control level involving verifying said user;

a second control level applying hack program detection tests to said access requests and verifying said user;

a third control level requiring use of predetermined download software for transmitting said access requests and verifying said user;

a fourth control level blocking access to said service on the basis of at least one communications address corresponding to said access requests; and

invoking said control levels sequentially depending on a number of failed attempts to verify said user.

15. An access control method as claimed in claim 14, wherein said user is verified by contacting a device with a known association to said user and said data processing apparatus, and having said user provide identification data using said device.

16. An access control system having components for executing the steps of the access control method as claimed in any one of the preceding claims.

17. Access control software stored on a computer system, having code for executing the steps of the access control method as claimed in any one of claims 1 to 15.

18. An access control system, including:

an access control server for receiving access requests for a service from a data processing apparatus, rate limiting access to the server until a user of said apparatus is verified, and sending to said data processing apparatus unique identification data; and

an IVR for contacting a device having an association with said data processing apparatus, issuing a request for said identification data, and providing the data received in response to said request to said access server in order to verify said user.

10/088034 - 082602

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 March 2001 (22.03.2001)

PCT

(10) International Publication Number
WO 01/20462 A1

(51) International Patent Classification[7]: G06F 12/14, 17/00, H04M 1/66

(21) International Application Number: PCT/AU00/01095

(22) International Filing Date:
13 September 2000 (13.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PQ 2787 13 September 1999 (13.09.1999) AU

(71) Applicant *(for all designated States except US)*: **TELSTRA R & D MANAGEMENT PTY LTD** [AU/AU]; 242 Exhibition Street, Melbourne, Victoria 3000 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HIBBERD, Timothy, Winston** [CA/AU]; 2/7 Bogota Avenue, Neutral Bay, New South Wales 2089 (AU).

(74) Agent: **WEBBER, David, Brian**; Davis Collison Cave, 1 Little Collins Street, Melbourne, Victoria 3000 (AU).

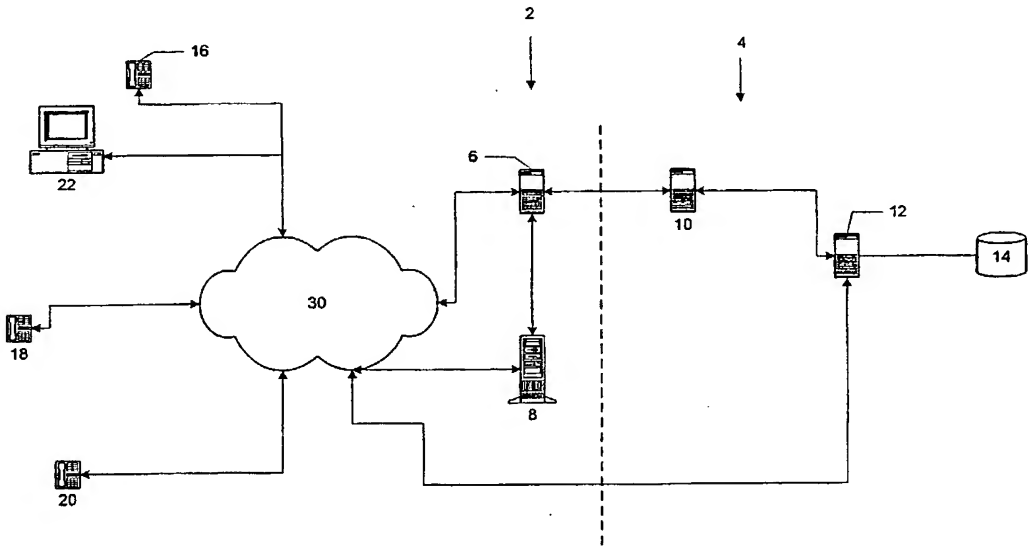
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AN ACCESS CONTROL METHOD



(57) Abstract: An access control method executed by a computer system, including applying an access rate limit until a user issuing access requests is verified, a first control level involving verifying the user, a second control level applying hack program detection tests to the access requests and verifying the user, a third control level requiring use of predetermined download software for transmitting the access requests and verifying the user, a fourth control level blocking access to the service on the basis of at least one communications address corresponding to the access requests, and invoking the control levels sequentially depending on a number of failed attempts to verify the user.

WO 01/20462 A1

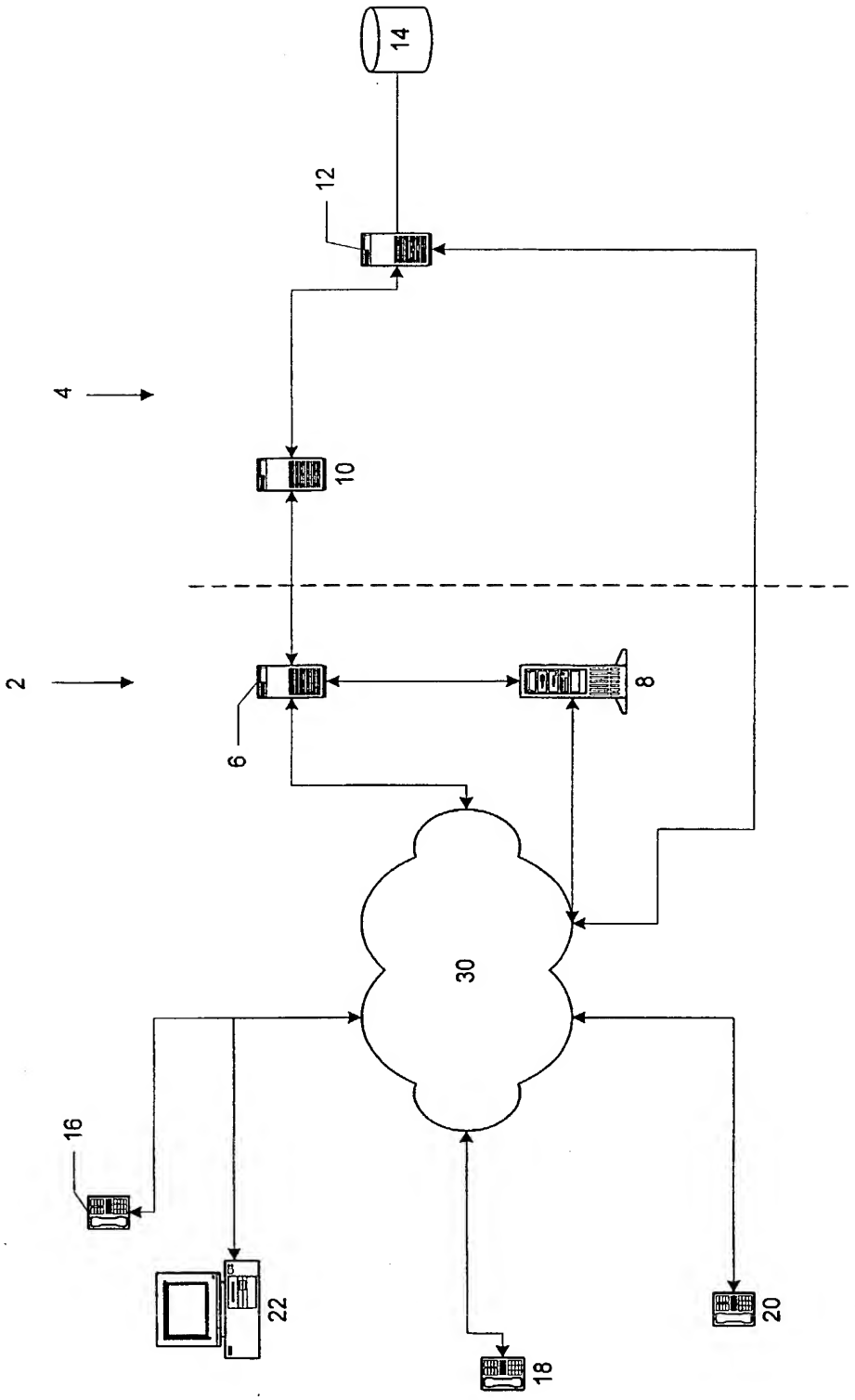


Figure 1

DECLARATION FOR PATENT APPLICATION

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled * An access control method

the specification of which

(Check one)
- ☐ is attached hereto
- ☐ was filed on _____ as Application Serial No. _____ and was amended on _____ (if applicable)

[x] International Patent Application No. PCT/AU00/01095 filed 13 September 2000

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the Patent Office all information known to me to be material to patentability as defined in 37 C.F.R. 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
PQ2787/99 (Number)	Australia (Country)	13 September 1999 (Day/Month/Year Filed)	[x] Yes	☐ No
PCT/AU00/01095 (Number)	PCT (Country)	13 September 2000 (Day/Month/Year Filed)	[x] Yes	☐ No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	☐ Yes	☐ No

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the Patent Office all information known to me to be material to patentability as defined in 37 C.F.R. 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

Direct all telephone calls to Michael A. Kaufman at (415) 781-1989.
Address all correspondence to:

FLEHR HOHBACH TEST
ALBRITTON & HERBERT LLP
Four Embarcadero Center - Suite 3400
San Francisco, California 94111-4187

File No. *

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, § 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first inventor:	1-00 * Timothy Winston HIBBERD
Inventor's signature:	Timothy Hibberd
Date:	July 14, 2002
Residence:	* 2/7 Bogota Avenue, Neutral Bay, New South Wales 2089, Australia AUX
Citizenship:	* Canadian
Post Office Address:	* " as above "

Full name of second joint inventor, if any:	*
Inventor's signature:	
Date:	
Residence:	*
Citizenship:	*
Post Office Address:	*

Full name of third joint inventor, if any:	*
Inventor's signature:	
Date:	
Residence:	*
Citizenship:	*
Post Office Address:	*

Full name of fourth joint inventor, if any:	*
Inventor's signature:	
Date:	
Residence:	*
Citizenship:	*